Hashed & Salted | A Privacy and Data Security Update
May 2022

Crypto, Blockchain and the Promise of Web3: Managing the Risk in Emerging Technologies

Blockchain-based technologies like cryptocurrencies, utility and non-fungible tokens, and decentralized networks are demanding more attention than ever. Over the last decade, cryptocurrency has evolved from facilitating underground dark web markets, to enabling unregulated capital raise programs during the Initial Coin Offering frenzy, and it is now emerging as a fundamental component of Web3 and its integrated digital economies. While serious questions about scalability, security and the regulatory landscape remain, many businesses may soon find undeniable value in these technologies.

The use of cryptocurrency presents a number of incentives and challenges for businesses. As more companies entertain adopting first- or third-party cryptocurrency solutions, it is important to ensure leadership and operational departments alike have a clear understanding of the considerations and risks associated with deploying an emerging technology. Below is an overview of some of the salient business risks present when developing and integrating cryptocurrency solutions.

Why Cryptocurrency?

Developers are realizing the opportunities that secure decentralization brings and are no doubt taking advantage of its functionality and ability to capture new markets and customers. Cryptocurrency users are generally more technologically savvy and encouraged by the promises of Web3, which include business transparency, personal privacy and digital rights. Sports betting and gaming companies are discovering new ways to increase user engagement through unique incentivization schemes. The travel industry is leveraging low-overhead loyalty programs that secondarily serve as customer-funded decentralized finance accounts.

As blockchain technologies advance, businesses may find that integrating cryptocurrency is useful for capturing the attention of younger audiences, accessing capital, streamlining payment systems and accounting departments, and becoming more active participants in the emerging digital economy. If the trends in development and engagement continue, many businesses should consider their medium- and long-term goals in light of the shift to digital payments and position themselves accordingly.

Understanding the Risks

For all the interesting use cases in development or yet to be imagined, blockchain-based programs and the teams that create them are still laying the groundwork. There are risks when usingany internet-connected technology, but particularly so with those in the early stages. Critical issues in security and infrastructure have yet to be fully addressed.

Attorney Advertising

Business Risks. In November 2021, nonstate-issued digital assets reached a combined market capitalization of $3 trillion, up from approximately $14 billion in early November 2016. While cryptocurrency's growth warrants attention, organizations should be cautious and cognizant of the market risks when accepting cryptocurrency. Volatility, liquidity, and manipulation and fraud continue to impact the value proposition of cryptocurrency for businesses. The cryptocurrency markets fluctuate wildly at times, entire platforms can evaporate overnight and newly issued digital currencies can be heavily influenced by fraudulent behavior.

Regulatory Risks. Regulatory frameworks are slowly falling into place. For example, over 30 cryptocurrency bills were introduced to Congress in 2021 alone. California's governor recently issued Executive Order N-9-22 to create a regulatory approach for cryptocurrency companies and to determine how to use blockchain technology for state and public institutions. The White House also recently issued an executive order titled "Ensuring Responsible Development of Digital Assets" with the intent to protect consumers, investors, businesses and global financial stability. But policymakers have yet to align on how to develop comprehensive guidance in the cryptocurrency space. Unclear or ill-fitting financial regulation governing the establishment and management of token-based economies, the raising of capital through public cryptocurrency distributions, and digital currency transactions raise legitimate concerns about businesses' ability to maintain compliance with an evolving patchwork of requirements.

A recent survey of 300 small-business owners found that 45% of those polled were not in favor of accepting cryptocurrency as payment, while another 33% were indifferent. Despite the potential upside to adopting digital currency, these figures are no surprise given the numerous instances of corporate misinterpretations and strategic missteps that have resulted in federal litigation and enforcement actions.

With potentially severe implications for noncompliance, businesses must carefully consider anti-money laundering (AML) and Know Your Customer (KYC) laws if transacting in digital currencies, particularly when accepting payments from foreign individuals or organizations. Businesses must also understand their obligations to avoid facilitating money laundering through domestic or foreign vendors that can represent the end of a complex and oftentimes obfuscated supply chain. The Office of Foreign Assets Control also requires businesses to verify that the source of any cryptocurrency the business accepts is not a sanctioned individual or entity.

Security Risks. Transmitting digital money and products on the internet within reach of bad actors anywhere in the world creates a number of challenges for businesses to consider. Chief among such challenges may be the Securities and Exchange Commission's (SEC) steady increase in the number of actions against SEC registrants and public companies for failing to maintain adequate cybersecurity controls. If you are evaluating a cryptocurrency product for your business, considering the resulting security requirements should be near the top of your priority list.

Second layer protocols (SLPs) are rapidly advancing to become the default tool for facilitating cryptocurrency transactions. SLPs are third-party applications built on top of foundational blockchains, like Bitcoin and Ethereum, to address the high costs and low speeds involved in many cryptocurrency transactions. Some anticipate SLPs will compete with and eventually antiquate traditional payment infrastructures like ACH and SWIFT. Of course, these protocols are not without risk. Transacting parties must rely on the third-party program to accurately and securely aggregate and record transactions on the blockchain. While the shift to aggregating transactions promises to reduce transaction delays and costs, some argue that the use of SLPs creates more opportunity for error and fraud and ultimately undermines the trust inherent in blockchain technologies.

Outsourcing and Vendor Risks. Many businesses have chosen to outsource cryptocurrency services in light of the overhead and risks associated with internally managed platforms. As with any outsourcing of financial services, businesses must properly audit their vendors' compliance and security posture. Do the vendors' operations conform with applicable privacy and cybersecurity, tax and accounting, and other financial services rules and regulations? Is the vendor properly licensed and compliant in the jurisdictions in which they (and you) operate? What level of integration is required, and what technical support does the vendor provide?

How to Protect Your Business and Data

- A secure wallet framework is critical to creating and nurturing a successful cryptocurrency economy. The recommended approach is to adopt a hot/cold program in which an internet-accessible software "hot" wallet is used to store limited operational funds that must be readily available to the business. "Cold" wallets, on the other hand, are hardware-based and should always be used for storing the bulk of an organization's funds.
- A $2 trillion cryptocurrency market attracts bad actors from around the world, and your business should be determined and practical about combating these risks by deploying adequate security controls, instituting employee cybersecurity training, and hiring or outsourcing experienced consultants to create, control and routinely audit programs, from creating, issuing and storing digital currency.
- It is important to understand and monitor your cryptocurrency data. Upstream association with transactions that facilitate money laundering, finance ransomware groups, and fund purchases of illegal goods and services may have investigators knocking at your door. Create systems to detect and address fraud. Keep a close eye on your transaction data, because others will too.
- Stay abreast of relevant cross-border issues and regulations and guidance in the financial services, privacy and cybersecurity, and intellectual property sectors.

Related Professional

Ryan Gallagher . . . . . rgallagher@loeb.com

6978 REV1 05-25-2022